HOGAN & HARTSON

Hogan & Hartson LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
+1.202.637.5600 **Tel**
+1.202.637.5910 **Fax**

www.hhlaw.com

Yaron Dori
Partner
+1.202.637.5458
ydori@hhlaw.com

February 21, 2008

Via ECFS

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 Twelfth Street, S.W., Suite TW-A325
Washington, D.C. 20554

Re: EB Docket No. 06-36 – Annual CPNI Compliance Certification

Dear Secretary Dortch:

SunCom Wireless, Inc., by its attorneys and pursuant to the Commission's January 29, 2008, *Public Notice* issued in the above-referenced proceeding (DA 08-171), hereby submits its attached CPNI Compliance Certification together with its accompanying "Statement Regarding SunCom Wireless, Inc., Customer Proprietary Network Information Operating Procedures."

This cover letter and the attached materials are intended to replace entirely SunCom's prior submission in this docket dated February 19, 2008.

Consistent with the requirements of the *Public Notice*, two copies of this submission are being delivered via U.S. mail to the Enforcement Bureau and one copy will be transmitted via e-mail to the Commission's copy contractor, Best Copy and Printing, Inc.

Kindly address any questions concerning this submission to the undersigned.

Respectfully submitted,

/Yaron Dori/

Yaron Dori

cc: Marcy Greene (Enforcement Bureau) (via U.S. Mail)
Best Copy and Printing, Inc. (via e-mail)
Joan Alexander (SunCom Wireless, Inc.)

ANNUAL 47 C.F.R. § 64.2009(e) CPNI CERTIFICATION

EB Docket No. 06-36

This certificate is provided pursuant to 47 C.F.R. § 64.2009(e) for the period from December 8, 2007, to December 31, 2007, which is the only period in calendar year 2007 during which the Commission's recently-promulgated revisions to its CPNI rules, which require the filing of this certificate, were in effect. A separate CPNI certification covering the January 1, 2007, through December 7, 2007, period was previously executed and has been maintained by the company.

Date Filed: February 21, 2008

Name of Company: SunCom Wireless, Inc.

Form 499 Filer ID: SunCom Wireless Operating Company, L.L.C. – 817978
SunCom Wireless Puerto Rico Operating Company, LLC – 825855

Name of Signatory: Eric Haskell

Title of Signatory: Executive Vice President & CFO

I, Eric Haskell, certify that I am an officer of the company named above and acting as an agent of the company, and that, to the best of my personal knowledge, information and belief, based on diligent inquiry, the company has established operating procedures designed to ensure compliance with the Commission's CPNI rules contained in 47 C.F.R. §§ 64.2001, *et seq.*

Attached to this certification is an accompanying "Statement Regarding SunCom Wireless, Inc. Customer Proprietary Network Information Operating Procedures," which explains how the company's operating procedures during the above-referenced certification period were designed to maintain compliance with the CPNI rules.

The company has not taken any actions against data brokers during the above-referenced certification period, and the company is not aware of any activity by data brokers for which action should have been taken.

The company did not receive any customer complaints during the above-referenced certification period concerning the unauthorized release of subscriber CPNI.

Eric Haskell, Executive Vice President & CFO
SunCom Wireless, Inc.

STATEMENT REGARDING SUNCOM WIRELESS, INC.
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI)
OPERATING PROCEDURES

February 21, 2008

SunCom Wireless, Inc. ("SunCom" or "Company") provides this statement pursuant to 47 C.F.R. § 64.2009(e) to explain how SunCom's operating procedures were designed to ensure compliance with the Federal Communications Commission's ("Commission") CPNI rules for the period from December 8, 2007, to December 31, 2007.

Certification

SunCom requires an officer of the Company to sign and file with the Commission a compliance certification on an annual basis. The certification is based on the personal knowledge of the certifying officer, acquired through personal information and inquiry, that SunCom has established operating procedures designed to ensure compliance with the Commission's CPNI rules. SunCom's certifying officer relies in part upon information provided by corporate officers and managers directly responsible for implementing the Company's CPNI operating procedures.

Customer Approval to Use, Disclose, or Permit Access to CPNI

SunCom does not use, disclose, or permit access to its customers' CPNI except as such use, disclosure, or access is permitted without customer approval, or as otherwise provided in Section 222 of the Communications Act of 1934, as amended. Accordingly, the customer notice and associated record-keeping requirements of the Commission's CPNI rules are not applicable. Should SunCom change its policies such that the use, disclosure, or permitted access to CPNI requires customer approval, appropriate customer notice, record-keeping, and FCC notification practices will be implemented.

Consistent with the Commission's rules, although SunCom does not necessarily engage in each of the following activities, SunCom's policies permit it to use, disclose, or permit access to CPNI without customer approval for the purpose of:

- providing or marketing service offerings among the categories of service (*i.e.*, Commercial Mobile Radio Services (CMRS)) to which the customer already subscribes without customer approval;
- provisioning customer premises information (CPE) and information service(s);
- conducting research on the health effects of CMRS;
- marketing services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain centrex features;

- protecting the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; and

- as otherwise permitted in Section 222 of the Communications Act of 1934, as amended.

Notice of CPNI Rights

As explained above, SunCom does not use, disclose, or permit access to its customers' CPNI except as permitted without customer approval, or as otherwise provided in Section 222 of the Communications Act of 1934, as amended. Therefore, SunCom is not required to provide customer notice regarding CPNI rights as prescribed in the Commission's rules. Should SunCom change its policies such that customer notice is required, such notice will be provided.

Record Retention for Marketing Campaigns

SunCom maintains records of sales and marketing campaigns that use CPNI. Records include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. SunCom maintains such records for at least one year.

Reporting Opt Out Failures

SunCom's policy is to not use, disclose, or permit access to its customers' CPNI without customer approval except as permitted under the Commission's rules or as otherwise provided in Section 222 of the Communications Act of 1934, as amended. Should SunCom change its policies and seek customer approval to use, disclose, or permit access to CPNI, SunCom will provide written notice of opt-out failures to the Commission within five business days as specified in the Commission's rules.

Supervisory Review Process

SunCom has a supervisory review process that governs its use of CPNI. As a general matter, employees must receive permission from their supervisors or other authorized personnel before using or disclosing CPNI for sales or marketing purposes.

Safeguarding CPNI

SunCom takes the privacy and security of CPNI seriously. In addition to its internal policies, which are designed to ensure compliance with the Commission's CPNI Rules, SunCom publishes online its Terms & Conditions of service, which explains how SunCom uses, discloses, and protects customer information, including CPNI, consistent with applicable law.

General Privacy and Security Measures

SunCom has implemented numerous controls to ensure compliance with the FCC's CPNI rules. For example, SunCom has in place a team of employees whose responsibilities focus on,

among other things, CPNI protection and compliance. Additionally, CPNI released to SunCom's sales agents is specifically protected from disclosure through confidentiality provisions contained in SunCom's dealer agreement with its agents. SunCom agents must protect CPNI in their possession from unauthorized disclosure and must advise their employees, sub-agents, and similar individuals of their obligation to protect the CPNI. Additionally, the confidentiality provisions of the dealer agreement by their terms survive any termination of the dealer agreement. SunCom also undertakes other privacy precautions through its electronic data retention policy, such as removing historical billing information from its central customer database after a certain period of time.

Customer Authentication Procedures

SunCom has established procedures that require proper authentication prior to disclosing CPNI based on customer-initiated telephone contacts, in-store visits, and online. SunCom does not disclose call detail information over the telephone in response to customer-initiated telephone contacts unless the customer provides a previously-established Personal Identification Number or "PIN" that is not prompted by SunCom requesting readily available biographical or account information. If SunCom cannot authenticate a customer through the PIN process, SunCom either will randomly-generate and transmit a PIN via SMS text message to the telephone number of record and have the customer confirm the PIN once it is received before disclosing call detail information on a customer-initiated call, or SunCom will disclose call detail information only by calling the customer at the telephone number of record or by transmitting the information to the address of record. SunCom requires a valid government-issued photo ID matching the customer's account information prior to disclosing CPNI during a visit to a retail store. Online account access to CPNI is permitted only with a password – initially established through use of a randomly-generated PIN delivered to the customer by means of an SMS text message to the telephone number of record. SunCom also provides optional account passwords outside the online environment (e.g., for calls to customer care); but if these passwords are established using customer biographical information, they are not used as an authentication method by SunCom for the release of call detail CPNI to end users.

Employee Training Program

SunCom provides Company-wide training to educate and train its personnel regarding the confidentiality of customer information, including authorized and unauthorized uses of CPNI. As part of their training, employees are provided with a document titled "CPNI 101," which explains CPNI and SunCom's policies regarding the proper use and safeguarding of CPNI. Employees must acknowledge that they have read the training document. In addition, all SunCom employees must affirmatively acknowledge, on an annual basis, that they have received and agree to abide by SunCom's Professional and Business Code of Conduct, which is incorporated as part of the employee handbook. The Code of Conduct explains that all customer information, including CPNI, must be maintained in the strictest of confidence and may not be disclosed except as authorized and necessary when performing duties for SunCom.

Employee Discipline Program

SunCom has a disciplinary process in place to address noncompliance with Company policies, including policies concerning employee use of, access to, and disclosure of CPNI. An employee found to have violated SunCom's policies, including policies relating to use of, access to, and disclosure of CPNI, is subject to disciplinary action up to and including termination.

Notice of Account Changes

SunCom mails a notice to the customer's address of record within 48 business hours whenever, among other changes, a password for access to call detail CPNI, customer response to a back-up means of authentication for such lost or forgotten passwords, online account, or address of record is created or changed. Any notice sent to an address of record is sent only to an address associated with the customer's account for at least 30 days (except for accounts activated within the last 30 days, in which case the notice is sent to the address provided at account activation). Any such notice does not include or reveal the changed information.

Notice of Security Breaches

SunCom notifies law enforcement as soon as practicable, but in no event later than seven (7) business days after a reasonable determination has been made that a breach of its customer's CPNI has occurred. The notice process conforms to procedures established by the Commission and is otherwise in accordance with 47 C.F.R. § 64.2011.

SunCom strives to notify customers of the breach no sooner than the eighth business day following completion of the notice to law enforcement unless directed by the U.S. Secret Service or the FBI not disclose or notify customers. SunCom respects any agency request that SunCom not to disclose the breach for an initial period of up to 30 days, which may be extended further by the agency. The requesting agency must provide its direction in writing, as well as any notice that delay is no longer required.

Recordkeeping of Unauthorized Disclosures of CPNI, Customer Complaints, and Actions Taken Against Pretexting

A record of CPNI security breaches, notifications made to law enforcement, and notifications made to customers is maintained for at least two years.

Customer complaints concerning the unauthorized release of CPNI are reported and investigated internally, and are broken out by category of complaint (e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized). A summary of all such complaints in the prior year is included along with the annual certification to the Commission.

A record of any actions taken by SunCom against data brokers is maintained and an explanation of such actions included with the annual certification to the Commission, including any information SunCom has with respect to the processes pretexters are using to attempt to access CPNI.